PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-055731

(43)Date of publication of application : 25.02.1997

---

(51)Int.Cl. H04L 9/18

G09C 1/00

G11B 20/10

// G06F 12/14

---

(21)Application number : 07-206351 (71)Applicant : SONY CORP

(22)Date of filing : 11.08.1995 (72)Inventor : SAKO YOICHIRO

OSAWA YOSHITOMO

KURIHARA AKIRA

KAWASHIMA ISAO

YONEYAMA SHIGEYUKI

---

(54) SIGNAL TRANSMITTING METHOD, SIGNAL RECORDING MEDIUM, AND SIGNAL REPRODUCING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent illegal use and illegal copying by preventing reproduction form information such as copy administration information and charging information to be altered or modified.

SOLUTION: A reproduction form information adding circuit 14 in a header adding circuit 13 performs data conversion for ciphering for the reproduction form information such as copy administration information and charging information from a terminal 15 according to key information from a terminal 15K, and adds the converted information to data and transmits them. On a reproduction side, a reproduction form information detecting circuit 25 in a

header separating circuit 25 performs data conversion deciphering for the ciphered reproduction format information by using key information from a terminal 27K and the original reproduction format information is taken out of a terminal 27P.

LEGAL STATUS [Date of request for examination] 16.07.2002

[Date of sending the examiner's decision of rejection] 23.08.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection] 2005-18403

[Date of requesting appeal against examiner's decision of rejection] 22.09.2005

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] The signal-transmission approach characterized by performing data conversion according to the key information on encryption to the above-mentioned playback mode information in the signal-transmission approach of adding and transmitting playback mode information to an input signal.

[Claim 2] The above-mentioned playback mode information is the signal-transmission approach according to claim 1 characterized by including either [at least] copy management information or accounting information.

[Claim 3] The above-mentioned data conversion is the signal-transmission approach according to claim 1 characterized by being carried out by the logical operation of the data of the above-mentioned playback mode information, and

the key information on encryption.

[Claim 4] The key information on the above-mentioned encryption is the signal-transmission approach according to claim 1 characterized by including address information at least in a part.

[Claim 5] The above-mentioned playback mode information is the signal-transmission approach according to claim 1 characterized by being arranged in the location specified using position assignment information.

[Claim 6] The signal-transmission approach characterized by arranging the above-mentioned playback mode information in the location specified using position assignment information in the signal-transmission approach of adding and transmitting playback mode information to an input signal.

[Claim 7] The above-mentioned playback mode information is the signal-transmission approach according to claim 6 characterized by including either [at least] copy management information or accounting information.

[Claim 8] The signal record medium characterized by recording the signal acquired by performing data conversion according to the key information on encryption to the playback mode information added to an input signal, and changing.

[Claim 9] The above-mentioned playback mode information is a signal record medium according to claim 8 characterized by including either [at least] copy

management information or accounting information.

[Claim 10] The above-mentioned playback mode information is a signal record medium according to claim 8 characterized by being arranged in the location specified using position assignment information.

[Claim 11] The signal record medium characterized by arranging and recording the playback mode information added to an input signal on the location specified using position assignment information, and changing.

[Claim 12] The signal-regeneration equipment characterized by to have a key information input means is signal-regeneration equipment which reproduces the signal recorded by performing data conversion according to the key information on encryption to the playback mode information added to an input signal, and input the key information on the above-mentioned encryption, and a means perform data conversion for the decryption corresponding to the above-mentioned encryption according to the key information from this key information input means.

[Claim 13] The above-mentioned playback mode information is signal regeneration equipment according to claim 12 characterized by including either [at least] copy management information or accounting information.

[Claim 14] The above-mentioned playback mode information is signal regeneration equipment according to claim 12 characterized by being arranged

in the location specified using position assignment information.

[Claim 15] The signal-regeneration equipment which is signal-regeneration equipment which the playback mode information added to an input signal is arranged and recorded on the location specified using position assignment information, and reproduces a signal, and is characterized by to have the means which takes out the playback mode information on the location specified using the above-mentioned tab-control-specification information.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the anti-copying of a signal and the inhibition of an unauthorized use by which transmission or record playback is carried out or the signal-transmission approach applicable to an accounting system, a signal record medium, and signal regeneration equipment.

[0002]

[Description of the Prior Art] In recent years, anti-copying and inhibition of an unauthorized use have been made important by large-capacity-izing and spread

of a digital recording medium of optical disks etc. That is, since the duplicate object which does not have degradation by the copy or dubbing can be generated easily in the case of digital audio data or a digital video data and the same data as the original data can copy to it easily in the case of computer data, it is the actual condition which evils, such as infringement of the copyright by the illegal copy, are already producing.

[0003] Since it is such, specification which records the information for illegal copy prevention on an original data-logging medium for the purpose of prevention of the above-mentioned illegal copy is proposed, and it is used.

[0004] for example, as a method for the above-mentioned illegal copy prevention in the digital audio signal record regenerative apparatus called the so-called R-DAT (Rotary head Digital Audio Taperecoder) To the Maine data area of the digital audio signal recorded on the digital audio tape as a signal record medium The prohibition code (the so-called SCMS: prohibition code of the specification of a serial copy managerial system) for forbidding prohibition and the gradual generation copy of a digital copy (namely, generation limit) is recorded. When a digital audio signal recording apparatus detects this prohibition code, a method which forbids copy record of the digital audio signal concerned to a new digital audio tape top is adopted.

[0005] Moreover, since [which prevents the illegal copy of a digital video signal,

for example] it was recorded on the signal record medium, it considers recording the predetermined bit ID for illegal copy prevention (CGMS: prohibition code of the specification of a copy generation-control system) on an original digital recording medium like the method of the illegal copy prevention between the record regenerative apparatus in above-mentioned R-DAT.

[0006] Furthermore, in the case of computer data, the file content itself is enciphered using encryption key information, and only the user by whom normal was registered in it is given carrying out use consent. In addition, this distributes the digital recording medium by which information was enciphered and recorded as a gestalt of the distribution of information, pays a tariff for the contents which the user needed, receives key information, and is connected with a system which solves a code and is made available.

[0007]

[Problem(s) to be Solved by the Invention] However, a conventional prohibition code, cryptographic key information, etc. for signal record media which were mentioned above are recorded on the specific location of the system proper accessed by the user on a record medium, as shown in JP,5-173891,A.

[0008] Moreover, since it opts for the location and bit allocation on the record medium of data, playback mode information, such as copy management information and accounting information, has the problem of unauthorized use of

skipping, or altering and using it. That is, since playback mode information, such as copy management information and accounting information, is in an accessible location from a user, it tended to be set as the object of decode by the malicious user, or an illegal copy.

[0009] Moreover, there is a possibility that the arrangement of compatibility of the above-mentioned playback mode information may be lost in each encryption technique in the location of arbitration as it is fixed. Moreover, if playback mode information is arranged fixed, the technique of encryption will also be fixed, it may be lacking in flexibility and expandability and the own life of a format may be contracted.

[0010] This is considering as a problem, not only when transmitting record playback, transmission and reception, etc. of a digital signal, but when transmitting an analog signal.

[0011] This invention is made in view of the actual condition which was mentioned above, and it aims at offering the signal-transmission approach, a signal record medium, and signal regeneration equipment which make difficult an unauthorized use, an illegal copy, etc. by changing or altering playback mode information, such as copy management information and accounting information.

[0012]

[Means for Solving the Problem] In order to solve the above-mentioned technical

problem, this invention is characterized by performing data conversion according to the key information on encryption to the playback mode information added to the signal which it is going to transmit or record.

[0013] Here, as for playback mode information, it is desirable to arrange this playback mode information in the location specified using position assignment information including either [at least] copy management information or accounting information.

[0014] Moreover, this invention is characterized by arranging playback mode information in the location specified using position assignment information.

[0015] Since, as for the enciphered playback mode information, the contents are not understood without key information, it is hard to receive an alteration and an alteration. Moreover, it is made the location specified using tab-control-specification information by the ability not taking out easily by arranging playback mode information.

[0016]

[Embodiment of the Invention] It explains referring to a drawing about the gestalt of desirable operation of this invention hereafter.

[0017] Drawing 1 is the block diagram showing roughly an example of a configuration of that the gestalt of operation of this invention is applied. In this drawing 1 , digital data obtained by carrying out digital conversion of the audio

signal and video signal of an analog, such as data and computer data, are supplied to the input terminal 11. This input digital data is sent to the sector-ized circuit 12, and is sector-ized per predetermined amount-of-data unit, for example, 2048 bytes. The sector-ized data are sent to the header addition circuit 13, and the header data arranged at the head of each sector are added. This header data includes playback mode information so that it may mention later, and this playback mode information has at least one side of copy management information and accounting information. The playback mode information on origin or original is supplied to terminal 15P of the playback mode information addition circuit 14, and this playback mode information addition circuit 14 performs data conversion for encryption to the playback mode information on the agency describing above according to the key information from terminal 15K, and he is trying to add the changed playback mode information. The data from the header addition circuit 13 are sent to the error correcting code-ized circuit 16, perform data delay and a parity account, and add parity in this error correcting code-ized circuit 16. In the next modulation circuit 17, according to a predetermined modulation technique, 8 bit data are changed into the modulation data of a 16-channel bit, and it sends to the synchronous addition circuit 18. In the synchronous addition circuit 18, the synchronizing signal of the so-called pattern of the AUTOOBU rule which breaks the modulation regulation of the

above-mentioned predetermined modulation technique was added per predetermined amount of data, and it has taken out through the output terminal 19.

[0018] The output signal from an output terminal 19 is transmitted by sending to a recording head, recording on data-logging media, such as the shape of a disk, the shape of a tape, and a semi-conductor, or transmitting through communication media. The reproducing head is reproduced from a record medium, or it is received through communication media, and the transmitted signal is supplied to the input terminal 21 by the side of playback. The signal supplied to this input terminal 21 is the same as the signal outputted from an output terminal 19, if signal degradation by transmission etc. is disregarded.

[0019] The signal from an input terminal 21 is sent to the synchronous detector 22, and separation of the synchronizing signal added in the above-mentioned synchronous addition circuit 18 is performed. The digital signal from the synchronous detector 22 is sent to a demodulator circuit 23, and processing which restores to the modulation of the above-mentioned modulation circuit 17 is performed. Specifically, it is the processing which changes a 16-channel bit into 8-bit data. The digital data from a demodulator circuit 23 is sent to the error correction decryption circuit 24, and decryption processing as reverse processing of coding in the above-mentioned error correcting code-ized circuit

16 is performed. The data by which the error correction decryption was carried out are sent to the header separation circuit 25, and the header of the head part of each sector is separated. As mentioned above, data conversion of the encryption using key information is performed, and he is trying for the playback mode information in this header data to take out the playback mode information decrypted by the playback mode information detector 26 by performing data conversion for a code decryption using the key information from terminal 27K from terminal 27P. It is sent to the sector decomposition circuit 28, and is decomposed into the sector of the above-mentioned predetermined amount-of-data unit, and the remaining data with which the header was separated by the header separation circuit 25, and the so-called user data are taken out from an output terminal 29.

[0020] Here, drawing 2 shows the example of sector format, to 2048 bytes of user data area 41, 4 bytes of synchronous field 42, 16 bytes of header field 43, and 4 bytes of error detecting code (EDC) field 44 are added, and 1 sector is constituted. The error detecting code of the error detecting code field 44 consists of 32 bits, i.e., 4 bytes, of CRC sign generated to the user data area 41 and the header field 43. In the header field 43, each field of the layer (layer) 47 which shows which layer of CRC45 which is the so-called cyclic code, the playback mode information 46, and a multilayer disk it is, the address 48, and a reserve 49

is prepared.

[0021] The playback mode information 46 is 1 byte (8 bits), and has structure as shown in drawing 3 . In this drawing 3 , 8-bit playback mode information consists of the 4-bit copy management information 52 the low order side with the 4-bit accounting information 51 the high order side. The code and flag which show whether price for the file or program containing the sector concerned to be no charge (free), or view and listen as accounting information 51 is the need (pay per view) or the price for copying is the need (pay per copy) are mentioned. The 4-bit copy management information 52 is divided into the 2 more bits copy generation information 53 and 2-bit copy authorization / prohibition information 54. As 2-bit copy generation information 53, "00", for example Original, The 2nd generation, the 1st generation of a copy of "01" and a copy of "10", and "11" express the copy of the 3rd [or more] generation, respectively. As 2-bit copy authorization / prohibition information 54 "00" -- to two generations, the possibility of a copy and "10" express the possibility of a copy, and "11" expresses [a copy free-lancer and "01"] one generation of bans on a copy, respectively. [for example,]

[0022] In case [in which data are transmitted] it records in the case or transmits, he performs encryption processing according to predetermined key information, and he is trying to arrange this enciphered playback mode information in the

predetermined location of the above-mentioned sector header field 43, i.e., the location of the playback mode information 46, without origin [it consists of the above-mentioned accounting information 51 or the copy management information 52] using original playback mode information as it is.

[0023] Drawing 4 is drawing showing one example of performing data conversion for encryption using 8-bit key information to 8-bit playback mode information. That is, the playback mode information on the above-mentioned dimension or original is supplied to the input terminal 61 of this drawing 4 , and 8-bit key information is supplied to the input terminal 62. It is sent to the ExOR (exclusive OR) circuit 63, an exclusive OR is taken for every bit, and these 8-bit data serve as enciphered playback mode information which is 8 bits, and are taken out from an output terminal 64.

[0024] Thus, by performing encryption processing using key information, if there is no key information, the contents of the playback mode information on original are not understood, but illegal acts, such as an alteration of the contents and an alteration, can be prevented effectively.

[0025] Moreover, drawing 5 shows not only key information but the example which performs data conversion for encryption using 1 byte the 8 more-bit low order side of address information, for example, a sector address. That is, in the example of this drawing 5 , while the playback mode information on the

above-mentioned dimension or original is supplied to an input terminal 65 and 8-bit key information is supplied to an input terminal 66, 1 byte (8 bits) is supplied to the input terminal 67 the low order side of a sector address. By taking an exclusive OR for each [which is sent to the ExOR (exclusive OR) circuit 68, and corresponds] bit of every, three kinds of these 8 bit data serve as enciphered playback mode information which is 8 bits, and are taken out from an output terminal 69.

[0026] Thus, by using a part of sector address for data conversion for encryption, the playback mode information enciphered for every sector changes, and the prevention effectiveness of an alteration or an unauthorized use is heightened further.

[0027] In addition, data conversion for encryption may not be limited to the example of these drawing 4 and drawing 5 , may apply conversion using the so-called pseudo-random number of an M sequence, and may make the logical operation by AND, OR, ExOR, NAND and NOR, inverted arch circuits, these combinational circuits, etc. perform instead of an ExOR (exclusive OR) circuit. Moreover, the transposition which changes the location of data in addition to logical operation, the permutation which replaces the value of data can be used as the above-mentioned data conversion.

[0028] Next, drawing 6 shows the disk-like record media 101, such as an optical

disk as an example of a record medium. This disk-like record medium 101 has the center hole 102 in the center, and the lead-in groove (leadin) field 103 which turns into a TOC (table of contents) field which is a program management field from the inner circumference of this disk-like record medium 101 toward a periphery, the program field 104 where program data were recorded, and a program termination field and the so-called lead-out (lead out) field 105 are formed. In an audio signal or the optical disk for video signal playback, an audio and a video data are recorded on the above-mentioned program field 104, and this audio, hour entry of a video data, etc. are managed in the above-mentioned lead-in groove field 103.

[0029] Using the identification information written in fields other than program field 104 which is a data storage area as a part of above-mentioned key information is mentioned. Specifically, the identification information of the proper of medium manufacturing installations, such as identification information, for example, identification information, such as a serial number of a medium proper, manufacturer identification information, vender identification information or identification information of the proper of a recording apparatus or an encoder, a cutting machine, and La Stampa, is written in the lead-in groove field 103 which is a TOC field, and the lead-out field 105. What is necessary is just to use the above-mentioned identification information as key information for decoding a

code at the time of playback. Moreover, identification information is written in physically or chemically inside the lead-in groove field 103, this is read at the time of playback, and you may make it use as key information for decoding a code.

[0030] Moreover, the above-mentioned playback mode information is recorded on the location of arbitration, without fixing a record location, and writing in the tab-control-specification information for specifying the record location of the above-mentioned playback mode information as a predetermined field like the TOC field of the above-mentioned lead-in groove field 103 is mentioned. In this case, the record location of the above-mentioned playback mode information may be directly specified for the tab-control-specification information on a TOC field, and the pointer in data is specified and you may make it specify the record location of the above-mentioned playback mode information with this pointer for the tab-control-specification information on a TOC field.

[0031] That is, drawing 7 shows the example which directs the record location of playback mode information with the pointer 72 as tab-control-specification information in the TOC data area 71. In this drawing 7 , the pointer 71 for the record tab control specification of playback mode information consists of the sector-address information 73, the offset information 74, the byte-count information 75, and attribute information. The predetermined sector 76 is

specified using the sector-address information 73 on such a pointer 71, the byte count from the offset of the playback mode information 77 within this sector 76, i.e., the head location of a sector, to the playback mode information 77 is specified using the offset information 74, and the byte count of this playback mode information 77 very thing is specified using the byte-count information 75.

[0032] Thus, since the record location of playback mode information is not fixed, the situation in which playback mode information, such as copy management information, is extracted and changed from the same location can be effectively prevented by fixing the record location.

[0033] Although data conversion for the encryption using key information, the address, etc. is performed as this playback mode information was mentioned above, origin [it does not perform such data conversion] may use original playback mode information.

[0034] Moreover, you may make it use a selling agency identification number, a manufacturer identification number, a recording device identification number, etc. for the sector address of a pointer, offset, etc.

[0035] Although the above is an example in the case of transmitting a digital data signal, this invention is also applicable to transmission of an analog signal.

[0036] That is, drawing 8 shows the example by which playback mode information, especially copy management information were added to the analog

video signal.

[0037] In this drawing 8 , the so-called protection code signal 81 is mixed at the predetermined level period of the vertical blanking interval of an analog video signal. The level period which arranges this protection code signal 81 is the 283rdH in the 20th (H is level period)H and the even number field for example, in the odd number field. As the 8-bit data 85 which consist of the 14 bits data 82 and the 6-bit error detecting code (CRCC) 83, and follow the 6-bit header 84 in the 14-bit data 82 show the above-mentioned playback mode information, especially copy management information and this protection code signal 81 mentioned above, encryption processing is performed using key information.

[0038] Here as an example of the contents of data 85 which shows 8-bit playback mode information MSB (most significant bit)86 expresses copy prohibition "1" / authorization "0." The 2nd generation, the 1st generation of a copy [the following 2 bit 87 / a copy generation, "00",] of original and "01" and a copy of "10", and "11" express the copy of the 3rd [or more] generation, respectively, and 4 bit 88 by the side of low order expresses the category code of a device. [i.e.,]

[0039] Also in the case of such playback mode information on a video signal, by enciphering, if there is no key information, the contents are not understood but the alteration of the contents can be prevented.

[0040] In addition, this invention is not limited only to the example of the gestalt of operation mentioned above, and not only the application to record/playback of as opposed to a record medium but its thing applicable to transmission of a digital signal or an analog signal generally is natural. Moreover, playback mode information is not limited to the above-mentioned example, but can change various numbers of bits and contents, and you may make it also include information, such as the contents of the source, and copy hysteresis. In addition, modification various in the range which does not deviate from the summary of this invention is possible.

[0041]

[Effect of the Invention] Since data conversion according to the key information on encryption has been performed to the playback mode information added to the signal which it is going to transmit or record according to this invention, the contents cannot be understood without key information, but an alteration and an alteration can be prevented, and unjust listening, an illegal copy, etc. can be prevented effectively.

[0042] Furthermore, by arranging the enciphered playback mode information in the location specified using position assignment information, ejection of playback mode information can be made difficult and the unauthorized use prevention effectiveness can be heightened further.

[0043] Arranging the playback mode information which is not enciphered in the location specified using position assignment information also prevents from taking out playback mode information easily, and this can prevent the unjust use by the alteration of playback mode information etc.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing an example of the configuration which can apply the gestalt of operation of this invention.

[Drawing 2] It is drawing showing an example of sector format.

[Drawing 3] It is drawing showing an example of playback mode information.

[Drawing 4] It is drawing showing the example of the data-conversion circuit for encryption.

[Drawing 5] It is drawing showing other examples of the data-conversion circuit for encryption.

[Drawing 6] It is drawing showing an example of a data-logging medium.

[Drawing 7] It is drawing showing an example which specifies the record location of playback mode information with a pointer.

[Drawing 8] It is drawing for explaining the example which added playback mode information to the analog video signal.

[Description of Notations]

12 Sector-ized Circuit

13 Header Addition Circuit

14 Playback Mode Information Addition Circuit

15K, 27K Key information input terminal

16 Error Correcting Code-ized Circuit

17 Modulation Circuit

18 Synchronous Addition Circuit

22 Synchronizing Separator Circuit

23 Demodulator Circuit

24 Error Correction Decryption Circuit

25 Header Separation Circuit

26 Playback Mode Information Detector

28 Sector Decomposition Circuit

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－55731

(43)公開日　平成９年(1997)２月25日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/18			Ｈ０４Ｌ	9/00	６５１
Ｇ０９Ｃ	1/00	６６０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６６０Ｄ
Ｇ１１Ｂ	20/10		7736－5Ｄ	Ｇ１１Ｂ	20/10	Ｈ
// Ｇ０６Ｆ	12/14	３２０		Ｇ０６Ｆ	12/14	３２０Ｂ

審査請求　未請求　請求項の数15　ＯＬ　（全７頁）

(21)出願番号　特願平7－206351

(22)出願日　平成７年(1995)８月11日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　佐古　曜一郎
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　大澤　義知
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　栗原　章
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(74)代理人　弁理士　小池　晃　（外２名）

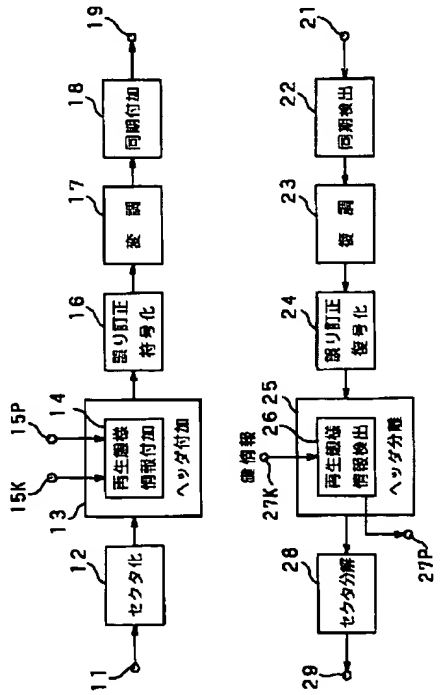
最終頁に続く

(54)【発明の名称】　信号伝送方法、信号記録媒体及び信号再生装置

(57)【要約】

【課題】　コピー管理情報や課金情報等の再生態様情報の改変や改竄を防止し、不正使用や不法コピーを防止する。

【解決手段】　ヘッダ付加回路１３内の再生態様情報付加回路１４により、端子１５Ｐからのコピー管理情報や課金情報等の再生態様情報に対して、端子１５Ｋからの鍵情報に応じて暗号化のためのデータ変換を施し、データに付加して伝送する。再生側では、ヘッダ分離回路２５内の再生態様情報検出回路２６により、暗号化された再生態様情報を、端子２７Ｋからの鍵情報を用いて暗号復号化のためのデータ変換を施し、元の再生態様情報を端子２７Ｐより取り出す。



1

【特許請求の範囲】

【請求項１】　入力信号に再生態様情報を付加して伝送する信号伝送方法において、
上記再生態様情報に対して暗号化の鍵情報に応じたデータ変換を施すことを特徴とする信号伝送方法。

【請求項２】　上記再生態様情報は、コピー管理情報及び課金情報の少なくとも一方を含むことを特徴とする請求項１記載の信号伝送方法。

【請求項３】　上記データ変換は、上記再生態様情報のデータと暗号化の鍵情報との論理演算により行われることを特徴とする請求項１記載の信号伝送方法。

【請求項４】　上記暗号化の鍵情報は、アドレス情報を少なくとも一部に含むことを特徴とする請求項１記載の信号伝送方法。

【請求項５】　上記再生態様情報は、所定の位置指定情報により指定される位置に配置されることを特徴とする請求項１記載の信号伝送方法。

【請求項６】　入力信号に再生態様情報を付加して伝送する信号伝送方法において、
上記再生態様情報を所定の位置指定情報により指定される位置に配置することを特徴とする信号伝送方法。

【請求項７】　上記再生態様情報は、コピー管理情報及び課金情報の少なくとも一方を含むことを特徴とする請求項６記載の信号伝送方法。

【請求項８】　入力信号に付加される再生態様情報に対して暗号化の鍵情報に応じたデータ変換を施して得られた信号が記録されて成ることを特徴とする信号記録媒体。

【請求項９】　上記再生態様情報は、コピー管理情報及び課金情報の少なくとも一方を含むことを特徴とする請求項８記載の信号記録媒体。

【請求項１０】　上記再生態様情報は、所定の位置指定情報により指定される位置に配置されることを特徴とする請求項８記載の信号記録媒体。

【請求項１１】　入力信号に付加される再生態様情報が所定の位置指定情報により指定された位置に配置されて記録されて成ることを特徴とする信号記録媒体。

【請求項１２】　入力信号に付加される再生態様情報に対して暗号化の鍵情報に応じたデータ変換を施して記録された信号を再生する信号再生装置であって、
上記暗号化の鍵情報を入力する鍵情報入力手段と、
この鍵情報入力手段からの鍵情報に応じて上記暗号化に対応する復号化のためのデータ変換を施す手段とを有することを特徴とする信号再生装置。

【請求項１３】　上記再生態様情報は、コピー管理情報及び課金情報の少なくとも一方を含むことを特徴とする請求項１２記載の信号再生装置。

【請求項１４】　上記再生態様情報は、所定の位置指定情報により指定される位置に配置されることを特徴とする請求項１２記載の信号再生装置。

2

【請求項１５】　入力信号に付加される再生態様情報が所定の位置指定情報により指定された位置に配置されて記録されて信号を再生する信号再生装置であって、
上記位置指定情報により指定された位置の再生態様情報を取り出す手段を有することを特徴とする信号再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、伝送あるいは記録再生される信号のコピー防止や不正使用の阻止、あるいは課金システムに適用可能な信号伝送方法、信号記録媒体、及び信号再生装置に関する。

【０００２】

【従来の技術】近年において、光ディスク等のディジタル記録媒体の大容量化と普及により、コピー防止や不正使用の阻止が重要とされてきている。すなわち、ディジタルオーディオデータやディジタルビデオデータの場合には、コピーあるいはダビングにより劣化のない複製物を容易に生成でき、また、コンピュータデータの場合には、元のデータと同一のデータが容易にコピーできるため、既に不法コピーによる著作権の侵害等の弊害が生じてきているのが実情である。

【０００３】このようなことから、上記不法コピーの防止を目的として、オリジナルのデータ記録媒体に、不法コピー防止のための情報を記録するような規格が提案され用いられている。

【０００４】例えば、いわゆるＲ－ＤＡＴ（Rotary head Digital Audio Taperecoder）と称されるディジタルオーディオ信号記録再生装置における上記不法コピー防止のための方式としては、信号記録媒体としてのディジタルオーディオテープ上に記録されるディジタルオーディオ信号のメインデータエリアに、ディジタルコピーの禁止や段階的な世代コピーを禁止（すなわち世代制限）するための禁止コード（いわゆるＳＣＭＳ：シリアルコピー管理システムの規格の禁止コード）を記録しておき、ディジタルオーディオ信号記録装置がこの禁止コードを検出したときに、新たなディジタルオーディオテープ上への当該ディジタルオーディオ信号のコピー記録を禁止するような方式が採用されている。

【０００５】また、信号記録媒体に記録された例えばディジタルビデオ信号の不法コピーを防止するために、上記Ｒ－ＤＡＴにおける記録再生装置間での不法コピー防止の方式と同様に、オリジナルのディジタル記録媒体に不法コピー防止のための所定のＩＤビット（ＣＧＭＳ：コピー世代管理システムの規格の禁止コード）を記録することが考えられている。

【０００６】さらに、コンピュータデータの場合には、ファイル内容自体を暗号化鍵情報を用いて暗号化し、それを正規の登録された使用者にのみ使用許諾することが行われている。なおこれは、情報流通の形態として、情

報が暗号化されて記録されたディジタル記録媒体を配布しておき、使用者が必要とした内容について料金を払って鍵情報を入手し、暗号を解いて利用可能とするようなシステムに結び付くものである。

【０００７】

【発明が解決しようとする課題】ところが、上述したような従来の信号記録媒体用の禁止コードや暗号鍵情報等は、特開平５－１７３８９１号公報に示されるように、記録媒体上のユーザからアクセスされるシステム固有の特定の場所に記録されている。

【０００８】また、コピー管理情報や課金情報等の再生態様情報は、データの記録媒体上の位置やビットアロケーションが決定されているため、読み飛ばしたり、改竄して使用したりするという不正使用の問題がある。すなわち、コピー管理情報や課金情報等の再生態様情報は、例えばユーザからアクセス可能な場所にあるため、悪意のあるユーザによる解読や不法コピーの対象になりやすかった。

【０００９】また、上記再生態様情報の配置がそれぞれの暗号化手法において任意の場所で固定的であると、互換性がなくなる虞れがある。また、再生態様情報を固定的に配置すれば、暗号化の手法も固定化されることになり、柔軟性，拡張性に乏しく、フォーマット自身の寿命を縮めてしまう可能性がある。

【００１０】これは、ディジタル信号の記録再生や送受信等の伝送を行う場合のみならず、アナログ信号を伝送する場合にも問題とされることである。

【００１１】本発明は上述したような実情に鑑みてなされたものであり、コピー管理情報や課金情報等の再生態様情報を改変したり改竄したりすることによる不正使用や不法コピー等を困難にするような信号伝送方法、信号記録媒体及び信号再生装置を提供することを目的とする。

【００１２】

【課題を解決するための手段】上記の課題を解決するために、本発明は、伝送あるいは記録しようとする信号に付加される再生態様情報に対して、暗号化の鍵情報に応じたデータ変換を施すことを特徴としている。

【００１３】ここで、再生態様情報は、コピー管理情報及び課金情報の少なくとも一方を含むものであり、この再生態様情報を所定の位置指定情報により指定される位置に配置することが好ましい。

【００１４】また、本発明は、再生態様情報を所定の位置指定情報により指定される位置に配置することを特徴としている。

【００１５】暗号化された再生態様情報は、鍵情報がなければ内容がわからないため、改変や改竄を受けにくい。また、位置指定情報によって指定された位置に再生態様情報を配置することで、容易に取り出せなくする。

【００１６】

【発明の実施の形態】以下、本発明の好ましい実施の形態について図面を参照しながら説明する。

【００１７】図１は、本発明の実施の形態が適用される構成の一例を概略的に示すブロック図である。この図１において、入力端子１１には、例えばアナログのオーディオ信号やビデオ信号をディジタル変換して得られたデータやコンピュータデータ等のディジタルデータが供給されている。この入力ディジタルデータは、セクタ化回路１２に送られ、所定データ量単位、例えば２０４８バイト単位でセクタ化される。セクタ化されたデータは、ヘッダ付加回路１３に送られて、各セクタの先頭に配置されるヘッダデータが付加される。このヘッダデータは、後述するように再生態様情報を含んでおり、この再生態様情報は、コピー管理情報と課金情報との少なくとも一方を有している。元のあるいはオリジナルの再生態様情報は、再生態様情報付加回路１４の端子１５Ｐに供給されており、この再生態様情報付加回路１４は、端子１５Ｋからの鍵情報に応じて上記元の再生態様情報に対して暗号化のためのデータ変換を施し、変換された再生態様情報を付加するようにしている。ヘッダ付加回路１３からのデータは誤り訂正符号化回路１６に送られ、この誤り訂正符号化回路１６では、データ遅延及びパリティ計算を行ってパリティを付加する。次の変調回路１７では、所定の変調方式に従って、例えば８ビットデータを１６チャンネルビットの変調データに変換し、同期付加回路１８に送る。同期付加回路１８では、上記所定の変調方式の変調規則を破る、いわゆるアウトオブルールのパターンの同期信号を所定のデータ量単位で付加し、出力端子１９を介して取り出している。

【００１８】出力端子１９からの出力信号は、例えば記録ヘッドに送ってディスク状やテープ状あるいは半導体等のデータ記録媒体に記録したり、通信媒体を介して送信したりすることにより伝送される。伝送された信号は、例えば再生ヘッドにより記録媒体から再生されたり、通信媒体を介して受信されたりして、再生側の入力端子２１に供給される。この入力端子２１に供給される信号は、伝送による信号劣化等を無視すれば出力端子１９から出力される信号と同じものである。

【００１９】入力端子２１からの信号は、同期検出回路２２に送られて、上記同期付加回路１８で付加された同期信号の分離が行われる。同期検出回路２２からのディジタル信号は、復調回路２３に送られて、上記変調回路１７の変調を復調する処理が行われる。具体的には、１６チャンネルビットを８ビットのデータに変換するような処理である。復調回路２３からのディジタルデータは、誤り訂正復号化回路２４に送られて、上記誤り訂正符号化回路１６での符号化の逆処理としての復号化処理が施される。誤り訂正復号化されたデータは、ヘッダ分離回路２５に送られて各セクタの先頭部分のヘッダが分離される。このヘッダデータ中の再生態様情報は、上述

したように鍵情報を用いた暗号化のデータ変換が施されており、再生態様情報検出回路２６により、端子２７Ｋからの鍵情報を用いて暗号復号化のためのデータ変換を施し、復号化された再生態様情報を端子２７Ｐより取り出すようにしている。ヘッダ分離回路２５によりヘッダが分離された残りのデータ、いわゆるユーザデータは、セクタ分解回路２８に送られて上記所定データ量単位のセクタに分解され、出力端子２９より取り出される。

【００２０】ここで、図２は、セクタフォーマットの具体例を示しており、１セクタは、２０４８バイトのユーザデータ領域４１に対して、４バイトの同期領域４２と、１６バイトのヘッダ領域４３と、４バイトの誤り検出符号（ＥＤＣ）領域４４とが付加されて構成されている。誤り検出符号領域４４の誤り検出符号は、ユーザデータ領域４１及びヘッダ領域４３に対して生成される３２ビットすなわち４バイトのＣＲＣ符号から成っている。ヘッダ領域４３内には、いわゆる巡回符号であるＣＲＣ４５、再生態様情報４６、多層ディスクのどの層かを示す層（レイヤ）４７、アドレス４８、予備４９の各領域が設けられている。

【００２１】再生態様情報４６は、例えば、１バイト（８ビット）で、図３に示すような構造を有している。この図３において、８ビットの再生態様情報は、上位側４ビットの課金情報５１と、下位側４ビットのコピー管理情報５２とから成っている。課金情報５１としては、当該セクタを含むファイルあるいはプログラムが、無料（フリー）であるか、視聴するための代金が必要（pay per view）であるか、コピーするための代金が必要（pay per copy）であるか等を示すコードやフラグが挙げられる。４ビットのコピー管理情報５２は、さらに２ビットのコピー世代情報５３と２ビットのコピー許可／禁止情報５４とに分割されている。２ビットのコピー世代情報５３としては、例えば“00”がオリジナル、“01”がコピーの１世代目、“10”がコピーの２世代目、“11”が３世代目以上のコピーをそれぞれ表し、２ビットのコピー許可／禁止情報５４としては、例えば、“00”がコピーフリー、“01”が２世代までコピーが可能、“10”が１世代のみコピーが可能、“11”がコピー禁止をそれぞれ表している。

【００２２】データを伝送する際、例えば記録したり送信したりする際には、上記課金情報５１やコピー管理情報５２から成る元のあるいはオリジナルの再生態様情報をそのまま用いずに、所定の鍵情報に応じた暗号化処理を施して、この暗号化された再生態様情報を上記セクタヘッダ領域４３の所定位置すなわち再生態様情報４６の位置に配置するようにしている。

【００２３】図４は、８ビットの再生態様情報に対して８ビットの鍵情報を用いて暗号化のためのデータ変換を施す一具体例を示す図である。すなわち、この図４の入力端子６１には上記元のあるいはオリジナルの再生態様情報が供給され、入力端子６２には８ビットの鍵情報が供給されている。これらの８ビットのデータは、ExOR（排他的論理和）回路６３に送られて各ビット毎に排他的論理和がとられ、８ビットの暗号化された再生態様情報となって出力端子６４より取り出される。

【００２４】このように、鍵情報を用いた暗号化処理を施すことにより、鍵情報がなければ元の再生態様情報の内容がわからず、内容の改変や改竄等の不法行為を有効に防止できる。

【００２５】また図５は、鍵情報のみならず、さらに８ビットのアドレス情報、例えばセクタアドレスの下位側１バイトを用いて暗号化のためのデータ変換を施す例を示している。すなわち、この図５の例では、入力端子６５に上記元のあるいはオリジナルの再生態様情報が供給され、入力端子６６に８ビットの鍵情報が供給されると共に、入力端子６７にセクタアドレスの下位側１バイト（８ビット）が供給されている。これらの３種類の８ビットデータは、ExOR（排他的論理和）回路６８に送られて対応する各ビット毎に排他的論理和がとられ、８ビットの暗号化された再生態様情報となって出力端子６９より取り出される。

【００２６】このように、セクタアドレスの一部を暗号化のためのデータ変換に用いることにより、セクタ毎に暗号化された再生態様情報が変化し、さらに改竄や不正使用の防止効果が高められる。

【００２７】なお、暗号化のためのデータ変換は、これらの図４、図５の例に限定されず、例えばいわゆるＭ系列の擬似乱数を用いて変換をかけてもよく、また、ExOR（排他的論理和）回路の代わりに、ＡＮＤ、ＯＲ、ＥｘＯＲ、ＮＡＮＤ、ＮＯＲ、インバート回路やこれらの組み合わせ回路等による論理演算を行わせてもよい。また論理演算以外に、データの位置を変える転置や、データの値を置き換える置換等も上記データ変換として使用できる。

【００２８】次に、図６は、記録媒体の一例としての光ディスク等のディスク状記録媒体１０１を示している。このディスク状記録媒体１０１は、中央にセンタ孔１０２を有しており、このディスク状記録媒体１０１の内周から外周に向かって、プログラム管理領域であるＴＯＣ（table of contents）領域となるリードイン（leadin）領域１０３と、プログラムデータが記録されたプログラム領域１０４と、プログラム終了領域、いわゆるリードアウト（lead out）領域１０５とが形成されている。オーディオ信号やビデオ信号再生用光ディスクにおいては、上記プログラム領域１０４にオーディオやビデオデータが記録され、このオーディオやビデオデータの時間情報等が上記リードイン領域１０３で管理される。

【００２９】上記鍵情報の一部として、データ記録領域であるプログラム領域１０４以外の領域に書き込まれた識別情報等を用いることが挙げられる。具体的には、T

ＯＣ領域であるリードイン領域１０３や、リードアウト領域１０５に、識別情報、例えば媒体固有の製造番号等の識別情報、製造元識別情報、販売者識別情報、あるいは、記録装置やエンコーダの固有の識別情報、カッティングマシンやスタンパ等の媒体製造装置の固有の識別情報を書き込むようにする。再生時には、上記識別情報を、暗号を復号するための鍵情報として用いるようにすればよい。また、リードイン領域１０３よりも内側に、物理的あるいは化学的に識別情報を書き込むようにし、これを再生時に読み取って、暗号を復号するための鍵情報として用いるようにしてもよい。

【００３０】また、上記再生態様情報を、記録位置を固定せずに任意の位置に記録するようにし、上記リードイン領域１０３のＴＯＣ領域のような所定領域に、上記再生態様情報の記録位置を指定するための位置指定情報を書き込んでおくことが挙げられる。この場合、ＴＯＣ領域の位置指定情報で直接的に上記再生態様情報の記録位置を指定してもよく、また、ＴＯＣ領域の位置指定情報ではデータ中のポインタが指定され、このポインタによって上記再生態様情報の記録位置を指定するようにしてもよい。

【００３１】すなわち、図７は、ＴＯＣデータ領域７１内の位置指定情報としてのポインタ７２により再生態様情報の記録位置を指示する例を示している。この図７において、再生態様情報の記録位置指定用のポインタ７１は、セクタアドレス情報７３、オフセット情報７４、バイト数情報７５及び属性情報から成っている。このようなポインタ７１のセクタアドレス情報７３により所定のセクタ７６が指定され、このセクタ７６内での再生態様情報７７のオフセット、すなわちセクタの先頭位置から再生態様情報７７までのバイト数がオフセット情報７４により指定され、この再生態様情報７７自体のバイト数がバイト数情報７５により指定される。

【００３２】このように、再生態様情報の記録位置が固定されないため、記録位置が固定されていることにより同じ位置からコピー管理情報等の再生態様情報が抜き出されて改変されるような事態を、有効に防止することができる。

【００３３】この再生態様情報は、上述したように鍵情報やアドレス等を用いた暗号化のためのデータ変換が施されているものであるが、このようなデータ変換を施さない元のあるいはオリジナルの再生態様情報を用いてもよい。

【００３４】また、ポインタのセクタアドレスやオフセット等に、販売元識別番号、製造者識別番号、記録装置識別番号等を用いるようにしてもよい。

【００３５】以上はディジタルデータ信号の伝送を行う場合の例であるが、本発明をアナログ信号の伝送に適用することもできる。

【００３６】すなわち、図８は、アナログビデオ信号に再生態様情報、特にコピー管理情報が付加された例を示している。

【００３７】この図８において、アナログビデオ信号の垂直帰線消去期間の所定の水平期間に、いわゆるプロテクトコード信号８１を混合している。このプロテクトコード信号８１を配置する水平期間は、例えば奇数フィールドでは２０Ｈ目（Ｈは水平期間）、偶数フィールドでは２８３Ｈ目である。このプロテクトコード信号８１は、例えば１４ビットのデータ８２と６ビットの誤り検出符号（ＣＲＣＣ）８３とから成っており、１４ビットのデータ８２内の６ビットのヘッダ８４に続く８ビットのデータ８５が上記再生態様情報、特にコピー管理情報を示すものであり、上述したように鍵情報を用いて暗号化処理が施されている。

【００３８】ここで、８ビットの再生態様情報を示すデータ８５の内容の具体例としては、ＭＳＢ（最上位ビット）８６がコピー禁止“１”／許可“０”を表し、次の２ビット８７がコピー世代、すなわち例えば“00”がオリジナル、“01”がコピーの１世代目、“10”がコピーの２世代目、“11”が３世代目以上のコピーをそれぞれ表し、下位側の４ビット８８が機器のカテゴリコードを表している。

【００３９】このようなビデオ信号の再生態様情報の場合にも、暗号化を施しておくことにより、鍵情報がなければ内容がわからず、内容の改変を防止できる。

【００４０】なお、本発明は、上述した実施の形態の例のみに限定されるものではなく、例えば、記録媒体に対する記録／再生への適用のみならず、一般にディジタル信号やアナログ信号の伝送に適用することができることは勿論である。また、再生態様情報は上記具体例に限定されず、ビット数や内容を種々変更可能であり、また、ソースの内容やコピー履歴等の情報も含めるようにしてもよい。この他、本発明の要旨を逸脱しない範囲で種々の変更が可能である。

【００４１】

【発明の効果】本発明によれば、伝送あるいは記録しようとする信号に付加される再生態様情報に対して、暗号化の鍵情報に応じたデータ変換を施しているため、鍵情報がなければ内容がわからず、改変や改竄を防止でき、不正聴取や不法コピー等を有効に防止できる。

【００４２】さらに、暗号化された再生態様情報を所定の位置指定情報により指定される位置に配置することにより、再生態様情報の取り出しを困難にして、不正使用防止効果をさらに高めることができる。

【００４３】これは、暗号化されていない再生態様情報を所定の位置指定情報により指定される位置に配置することでも、再生態様情報を容易に取り出せないようにし、再生態様情報の改変による不正な使用等を防止できる。

【図面の簡単な説明】

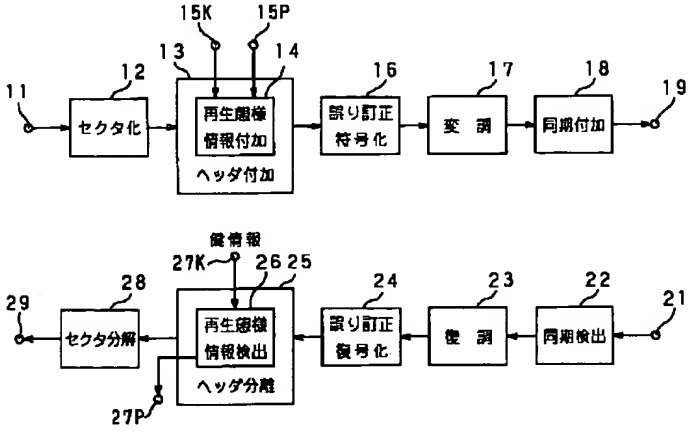
9　　10

【図１】本発明の実施の形態が適用可能な構成の一例を示すブロック図である。
【図２】セクタフォーマットの一例を示す図である。
【図３】再生態様情報の一例を示す図である。
【図４】暗号化のためのデータ変換回路の具体例を示す図である。
【図５】暗号化のためのデータ変換回路の他の具体例を示す図である。
【図６】データ記録媒体の一例を示す図である。
【図７】再生態様情報の記録位置をポインタにより指定する一例を示す図である。
【図８】アナログビデオ信号に再生態様情報を付加した具体例を説明するための図である。
【符号の説明】

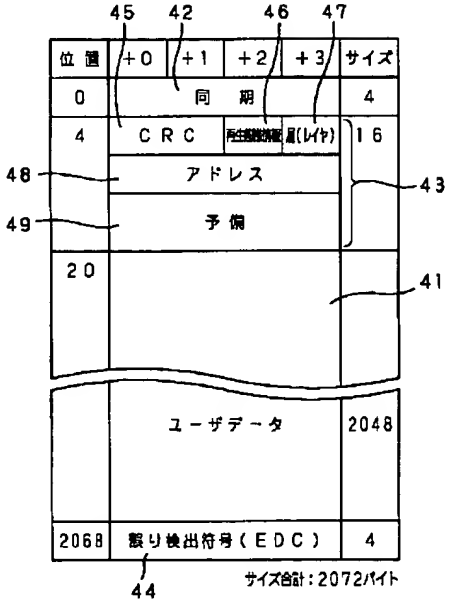
＊１２　セクタ化回路
１３　ヘッダ付加回路
１４　再生態様情報付加回路
１５Ｋ、２７Ｋ　鍵情報入力端子
１６　誤り訂正符号化回路
１７　変調回路
１８　同期付加回路
２２　同期分離回路
２３　復調回路
２４　誤り訂正復号化回路
２５　ヘッダ分離回路
２６　再生態様情報検出回路
２８　セクタ分解回路

＊

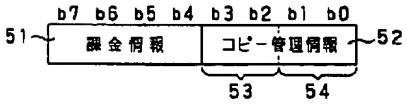
【図１】



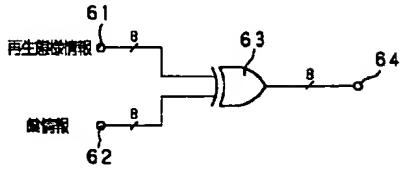
【図２】



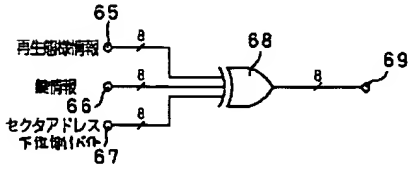
【図３】



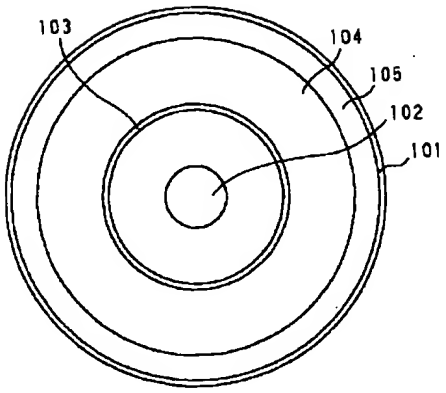
【図４】



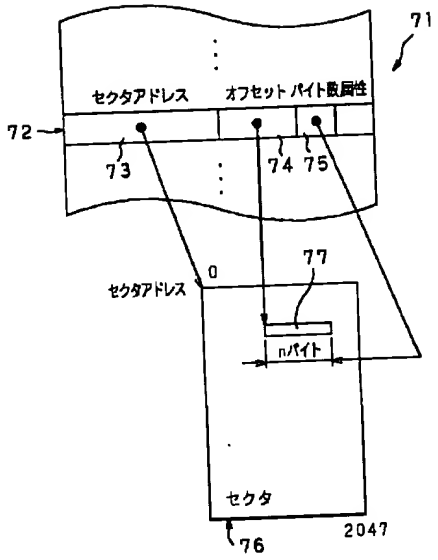
【図５】



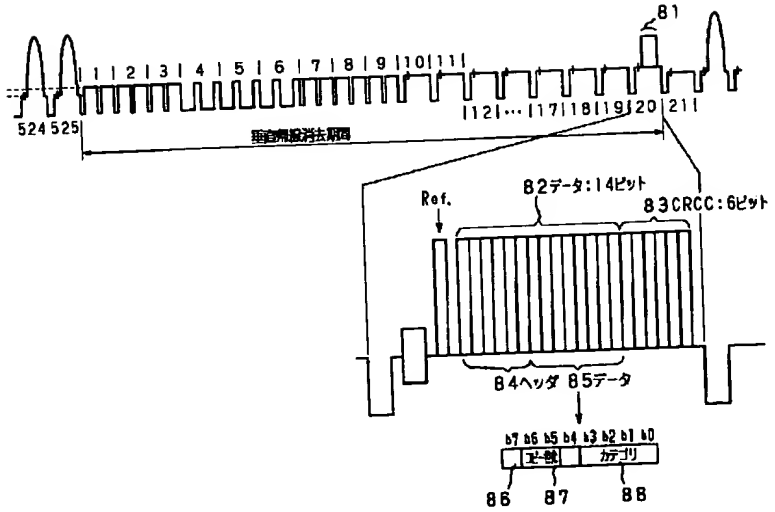
【図６】



【図７】



【図８】



フロントページの続き

(72)発明者　川嶋　功
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　米山　重之
東京都品川区北品川６丁目７番35号　ソニー株式会社内